

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MAINE**

IN THE MATTER OF THE SEARCH OF  
DEVICE(S) CONTROLLED BY MATTHEW  
BRACKLEY AND ASSOCIATED WITH  
TELEPHONE NUMBER (207) 837-1238  
UNDER RULE 41

No. 2:23-mj-00201-KFW

**AFFIDAVIT IN SUPPORT OF AN APPLICATION  
UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE**

I, **Kurt Ormberg**, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—any device(s) in the immediate control or on the person of Matthew Brackley at the time of his arrest and associated with telephone number (207) 837-1238 (hereinafter, the “TARGET DEVICE(S)”)—as described in Attachment A. Such a search would include an examination of the seized device for information described in Attachment B.

2. Unless otherwise noted, wherever in this affidavit I assert that a statement was made, that statement is described in substance and is not intended to be a verbatim recitation of such statement. Wherever in this affidavit I quote statements, those quotations have been taken from draft transcripts, which are subject to further revision.

3. Unless otherwise stated, the conclusions and beliefs I express in this affidavit are based on my training, experience, and knowledge of the investigation, and reasonable inferences I’ve drawn from my training, experience, and knowledge of the investigation.

**AFFIANT BACKGROUND**

4. I am a Special Agent assigned to the Federal Bureau of Investigation's Joint Terrorism Task Force (JTTF). I have been a Special Agent with the Federal Bureau of Investigation since March of 2005. Currently, I am tasked with investigating criminal activity in and around the Capitol grounds on January 6, 2021. Prior to 2005, I was a U.S. Capitol Police Officer for approximately three years. I have served twenty years in law enforcement during which time I have been assigned to, and/or supervised, a variety of units. Those units include FBI SWAT, FBI Safe Streets Task Force, FBI Crimes Against Children Task Force, FBI Violent Crime Task Force, FBI Child Abduction Rapid Deployment team and FBI JTTF. In these assignments, I initiated and/or supervised and/or assisted in numerous felony related investigations. I have been assigned to work on federal, state, and local criminal matters, as well international and domestic criminal and terrorism cases. I am familiar with and have participated in all of the normal methods of investigation, including, but not limited to, visual surveillance, interviewing of witnesses, the use of search and arrest warrants, the use of confidential human sources, the use of pen registers, the utilization of undercover agents, the use of Grand Jury, and the use of court-authorized wire and electronic intercepts. Additionally, I have consulted with other Agents and officers who have been involved in similar investigations.

5. As such, I am an "investigative or law enforcement officer" of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code. I am also a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C). As a

federal law enforcement officer, I am authorized to obtain and execute search warrants issued under the authority of the United States.

6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

7. Based on my training and experience and the facts set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. §§ 111(a) (assaulting, resisting, or impeding certain officers); 231(a)(3) (civil disorder); 1752(a)(1) (entering or remaining in restricted buildings or grounds); 1752(a)(2) (disorderly and disruptive conduct in a restricted building or grounds) and 40 U.S.C. §§ 5104(e)(2)(D) (disorderly or disruptive conduct in the Capitol Buildings) and 5104(e)(2)(G) (parading, demonstrating, or picketing in a Capitol Building) (the “TARGET OFFENSES”) have occurred. There is also probable cause to search the TARGET DEVICE(S), further described in Attachment A, for the things described in Attachment B.

#### **IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

8. The property to be searched is any device(s) in the immediate control or on the person of Matthew Brackley at the time of his arrest and associated with telephone number (207) 837-1238 (the “TARGET DEVICE(S)”).

9. The requested warrant would authorize the forensic examination of the TARGET DEVICE(S) for the purpose of identifying electronically stored data particularly described in **Attachment B**.

**PROBABLE CAUSE**

***Background – The U.S. Capitol on January 6, 2021***

10. U.S. Capitol Police (USCP), the FBI, and assisting law enforcement agencies are investigating a riot and related offenses that occurred at the United States Capitol Building, located at 1 First Street, NW, Washington, D.C., 20510 at latitude 38.88997 and longitude -77.00906 on January 6, 2021.

11. At the U.S. Capitol, the building itself has 540 rooms covering 175,170 square feet of ground, roughly four acres. The building is 751 feet long (roughly 228 meters) from north to south and 350 feet wide (106 meters) at its widest point. The U.S. Capitol Visitor Center is 580,000 square feet and is located underground on the east side of the Capitol. On the west side of the Capitol building is the West Front, which includes the inaugural stage scaffolding, a variety of open concrete spaces, a fountain surrounded by a walkway, two broad staircases, and multiple terraces at each floor. On the East Front are three staircases, porticos on both the House and Senate side, and two large skylights into the Visitor's Center surrounded by a concrete parkway. All of this area was barricaded and off limits to the public on January 6, 2021.

12. The U.S. Capitol is secured 24 hours a day by USCP. Restrictions around the U.S. Capitol include permanent and temporary security barriers and posts manned by USCP. Only authorized people with appropriate identification are allowed access inside the U.S. Capitol.

13. On January 6, 2021, the exterior plaza of the U.S. Capitol was closed to members of the public.

14. On January 6, 2021, a joint session of the United States Congress convened at the U.S. Capitol. During the joint session, elected members of the United States House of Representatives and the United States Senate were meeting in separate chambers of the U.S.

Capitol to certify the vote count of the Electoral College of the 2020 Presidential Election, which took place on November 3, 2020 (“Certification”). The joint session began at approximately 1:00 p.m. Eastern Standard Time (EST). Shortly thereafter, by approximately 1:30 p.m. EST, the House and Senate adjourned to separate chambers to resolve a particular objection. Vice President Mike Pence was present and presiding, first in the joint session, and then in the Senate chamber.

15. As the proceedings continued in both the House and the Senate, and with Vice President Mike Pence present and presiding over the Senate, a large crowd gathered outside the U.S. Capitol. As noted above, temporary and permanent barricades were in place around the exterior of the U.S. Capitol building, and USCP were present and attempting to keep the crowd away from the Capitol building and the proceedings underway inside.

16. At around 1:00 p.m. EST, known and unknown individuals broke through the police lines, toppled the outside barricades protecting the U.S. Capitol, and pushed past USCP and supporting law enforcement officers there to protect the U.S. Capitol.

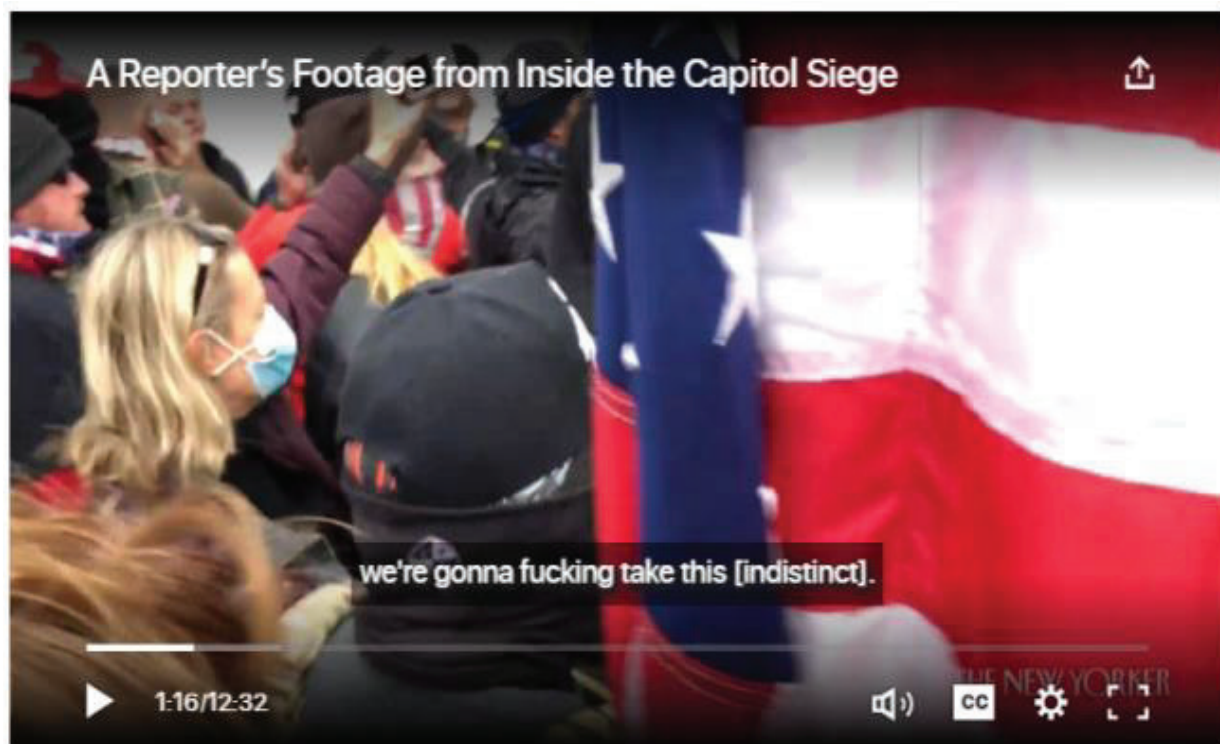
17. At around 1:30 p.m. EST, USCP ordered Congressional staff to evacuate the House Cannon Office Building and the Library of Congress James Madison Memorial Building in part because of a suspicious package found nearby. Pipe bombs were later found near both the Democratic National Committee and Republican National Committee headquarters.

18. Media reporting showed a group of individuals outside of the Capitol chanting, “Hang Mike Pence.” I know from this investigation that some individuals believed that Vice President Pence possessed the ability to prevent the certification of the presidential election and that his failure to do so made him a traitor.

19. At approximately 2:00 p.m. EST, some people in the crowd forced their way through, up, and over the barricades and law enforcement. The crowd advanced to the exterior

façade of the building. The crowd was not lawfully authorized to enter or remain in the building and, prior to entering the building, no members of the crowd submitted to security screenings or weapons checks by U.S. Capitol Police Officers or other authorized security officials. At such time, the certification proceedings were still underway and the exterior doors and windows of the U.S. Capitol were locked or otherwise secured. Members of law enforcement attempted to maintain order and keep the crowd from entering the Capitol.

20. Beginning shortly after 2:00 p.m. EST, individuals in the crowd forced entry into the U.S. Capitol, including by breaking windows and by assaulting members of law enforcement, as others in the crowd encouraged and assisted those acts. Publicly available video footage shows an unknown individual saying to a crowd outside the Capitol building, “We’re gonna fucking take this,” which your affiant believes was a reference to “taking” the U.S. Capitol.



21. Once inside, the subjects broke windows and doors, destroyed property, stole property, and assaulted federal police officers. Many of the federal police officers were injured and several were admitted to the hospital. The subjects also confronted and terrorized members of Congress, Congressional staff, and the media. The subjects carried weapons including tire irons, sledgehammers, bear spray, and tasers. They also took police equipment from overrun police including shields and police batons. At least one of the subjects carried a handgun with an extended magazine.

22. Between approximately 2:10 p.m. EST and 2:30 p.m. EST, Vice President Pence evacuated the Senate Chamber, and the Senate and House of Representatives were locked down and went into recess. Both the Senate and the House of Representatives Chamber were evacuated.

23. As the subjects attempted to break into the House Chamber, by breaking the windows on the chamber door, law enforcement were forced to draw their weapons to protect the victims sheltering inside. At around 2:45 p.m. EST, subjects broke into the office of House Speaker Nancy Pelosi.

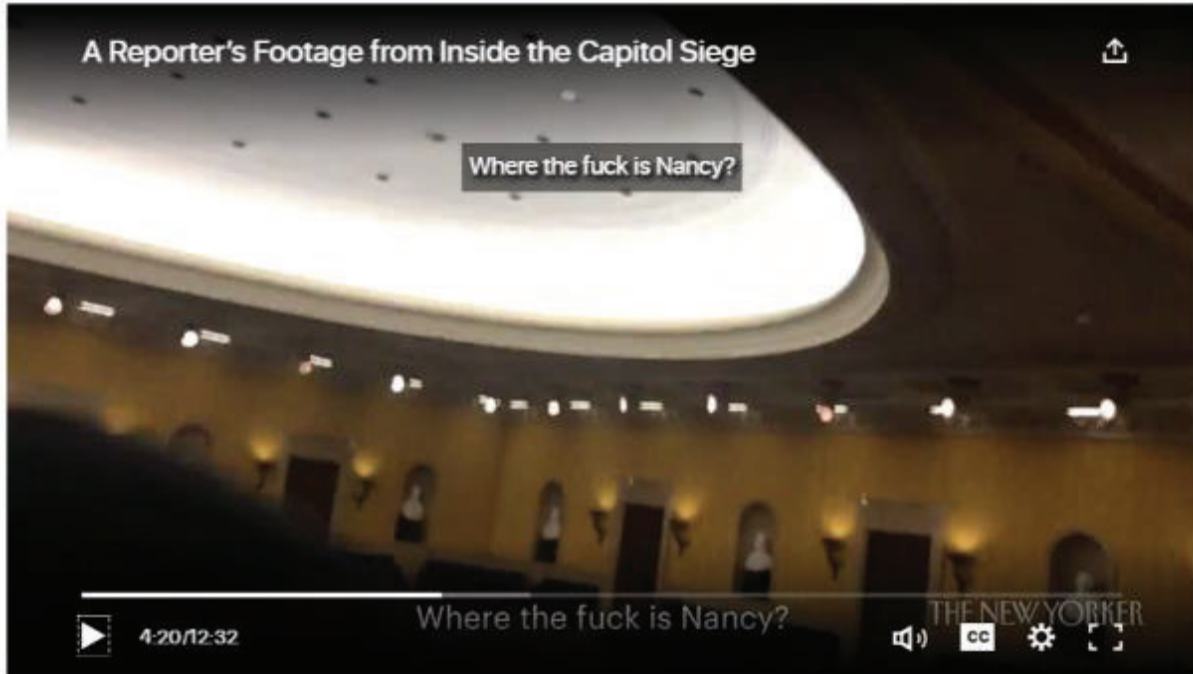
24. At around 2:47 p.m. EST, subjects broke into the Senate Chamber not long after it had been evacuated. Publicly available video shows an individual asking, "Where are they?" as they opened up the door to the Senate Chamber. Based upon the context, law enforcement believes that the word "they" is in reference to members of Congress.



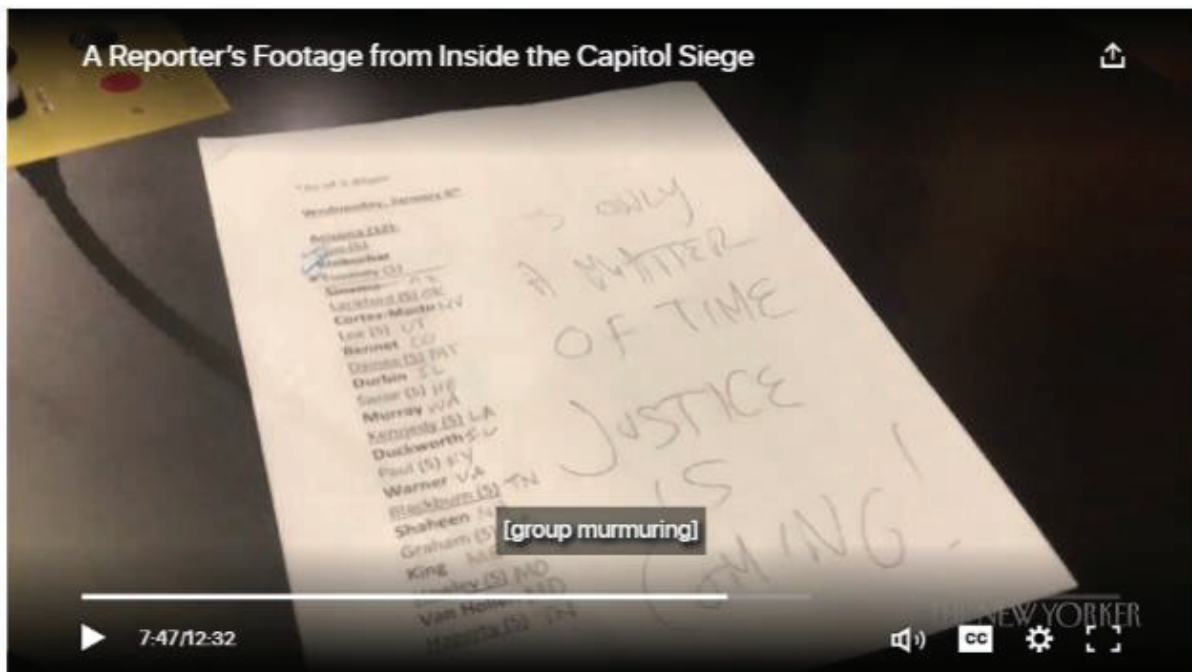


25. After subjects forced entry into the Senate Chamber, publicly available video shows that an individual asked, “Where the fuck is Nancy?” Based upon other comments and the context, law enforcement believes that the “Nancy” being referenced was the Speaker of the House of Representatives, Nancy Pelosi.





26. One subject left a note on the podium on the floor of the Senate Chamber. This note, captured by the filming reporter, stated “Its Only A Matter of Time Justice is Coming.”



27. During the time when the subjects were inside the Capitol building, multiple subjects were observed inside the U.S. Capitol wearing what appears to be, based upon my training

and experience, tactical vests and carrying flex cuffs. Based upon my knowledge, training, and experience, I know that flex cuffs are a manner of restraint that are designed to be carried in situations where a large number of individuals are expected to be taken into custody.





28. At around 2:48 p.m. EST, DC Mayor Muriel Bowser announced a citywide curfew beginning at 6:00 p.m. EST.

29. At around 2:45 p.m. EST, one subject was shot and killed while attempting to break into the House Chamber through the broken windows.

30. At about 3:25 p.m. EST, law enforcement officers cleared the Senate floor.

31. Between 3:25 and around 6:30 p.m. EST, law enforcement was able to clear the U.S. Capitol of all of the subjects.

32. Based on these events, all proceedings of the United States Congress, including the joint session, were effectively suspended until shortly after 8:00 p.m. EST the same day. In light of the dangerous circumstances caused by the unlawful entry to the U.S. Capitol, including the danger posed by individuals who had entered the U.S. Capitol without any security screening or weapons check, Congressional proceedings could not resume until after every unauthorized

occupant had left the U.S. Capitol and the building had been confirmed secured. The proceedings resumed at approximately 8:00 p.m. after the building had been secured. Vice President Pence remained in the United States Capitol from the time he was evacuated from the Senate Chamber until the session resumed.

33. Beginning around 8:00 p.m. EST, the Senate resumed work on the Certification.

34. Beginning around 9:00 p.m. EST, the House resumed work on the Certification.

35. Both chambers of Congress met and worked on the Certification within the Capitol building until approximately 3:00 a.m. EST on January 7, 2021.

36. During national news coverage of the aforementioned events, video footage which appeared to be captured on mobile devices of persons present on the scene depicted evidence of violations of local and federal law, including scores of individuals inside the U.S. Capitol building without authority to be there.

37. Based on my training and experience, I know that it is common for individuals to carry and use their cell phones during large gatherings, such as the gathering that occurred in the area of the U.S. Capitol on January 6, 2021. Such phones are typically carried at such gatherings to allow individuals to capture photographs and video footage of the gatherings, to communicate with other individuals about the gatherings, to coordinate with other participants at the gatherings, and to post on social media and digital forums about the gatherings.

38. Many subjects in news footage in the area of the U.S. Capitol are seen using cell phones in some capacity. It appears some subjects were recording the events occurring in and around the U.S. Capitol and others appear to be taking photos and/or video, to include photos and video of themselves after breaking into the U.S. Capitol itself, including photos of themselves damaging and stealing property. As reported in the news media, others inside and immediately



outside the U.S. Capitol live-streamed their activities, including those described above, as well as statements about these activities.

39. Photos below, available on various publicly available news, social media, and other media show some of the subjects within the U.S. Capitol during the riot. In several of these photos, the individuals who broke into the U.S. Capitol can be seen holding and using cell phones, including to take pictures and/or videos:



---

<sup>1</sup> <https://losangeles.cbslocal.com/2021/01/06/congresswoman-capitol-building-takeover-an-attempted-coup/>



<sup>2</sup> <https://www.businessinsider.com/republicans-objecting-to-electoral-votes-in-congress-live-updates-2021-1>.

<sup>3</sup> <https://www.thv11.com/article/news/arkansas-man-storms-capitol-pelosi/91-41abde60-a390-4a9e-b5f3-d80b0b96141e>

*Facts Specific to This Application – Identification of Matthew Brackley*

40. In June 2021, FBI Boston Field Office, Portland, Maine, Resident Office received a report, originating from the FBI Washington Field Office, which included a list of all 207 area code cellular numbers captured inside or on the grounds of the U.S. Capitol Building on January 6, 2021. The 207 area code is the sole area code assigned to the state of Maine. One number identified in that report was (207) 837-1238.

41. According to records obtained through a search warrant served on Google, two devices (Device #1 - Device ID 739512542 and Device #2 - Device ID 1998274199) associated with cellular number (207) 837-1238 were geo-located in the interior of the U.S. Capitol Building on January 6, 2021. Google estimates device location using sources including GPS data and information about nearby Wi-Fi access points and Bluetooth beacons. This location data varies in its accuracy, depending on the source(s) of the data. As a result, Google assigns a “maps display radius” for each location data point. Thus, where Google estimates that its location data is accurate to within 10 meters, Google assigns a “maps display radius” of 10 meters to the location data point. Finally, Google reports that its “maps display radius” reflects the actual location of the covered device approximately 68% of the time. In this case, Google location data shows that two devices associated with cell number (207) 837-1238 were within the U.S. Capitol between 2:26:56 PM EST and 3:06 PM EST on January 6, 2021.

42. Additionally, information obtained from Google via legal service identified that:

- a. Device #1 - Device ID 739512542 was associated with cellular number (207) 837-1238, email [mebrackley@gmail.com](mailto:mebrackley@gmail.com), and listed BRACKLEY as account holder. Device #1 listed a Google Account ID # of **977823091941**.



- b. Device #2 - Device ID 1998274199 was also associated with cellular number (207) 837-1238, as well as primary email [mattb@brackleyelectric.com](mailto:mattb@brackleyelectric.com), recovery email [mebrackley@gmail.com](mailto:mebrackley@gmail.com), and listed BRACKLEY as account holder. Device #2 listed a Google Account ID # of **363576324849**.

43. On or about January 2022, searches of state and local government databases as well as third party databases were conducted to identify BRACKLEY and/or cellular number (207) 837-1238. The search revealed one Matthew Brackley with a date of birth in 1983, social security number ending in 8319, Maine driver's license number 5210280, and home address in West Bath, Maine 04530.

44. FBI agents obtained BRACKLEY's driver's license photo from a law enforcement database and ran it against video footage from the U.S. Capitol on January 6, 2021. This returned numerous videos of BRACKLEY inside the U.S. Capitol on January 6, 2021, including third party footage taken from other rioters and news media and the Capitol's own Closed Circuit Television (CCTV). I have reviewed this footage.

45. On January 5, 2022, FBI agents interviewed BRACKLEY in person at his residence in West Bath, Maine. The agents present at this interview, including me, observed that BRACKLEY appeared to be the same individual present in the identified videos from the U.S. Capitol on January 6, 2021.

***Facts Specific to This Application –Brackley's Conduct on January 6***

46. On January 5, 2021, BRACKLEY emailed his senators imploring them to "stand up to this blatant corruption and support a second term for President Donald J. Trump," adding that "the people will." The same evening, BRACKLEY flew from Portland, Maine to Washington,

DC. The next morning, January 6, 2021, BRACKLEY attended the Stop the Steal rally on the National Mall.

47. After the rally, BRACKLEY walked to the U.S. Capitol, arriving on the West lawn at about 1:40 pm, where a large crowd was already gathered. BRACKLEY stood in the crowd near the Lower West Terrace, where a police line had formed to keep people from advancing towards the Capitol. In one video, BRACKLEY is seen on the Lower West Terrace as police deployed flashbang grenades into the crowd in an attempt to disburse it.

48. However, BRACKLEY did not leave U.S. Capitol Grounds, but instead approached a set of stairs underneath the scaffolding erected to construct the inaugural stage. Other rioters climbed onto the scaffolding and tore up the white tarp covering it, giving BRACKLEY and others greater access to the stairs. He and other rioters flooded the stairs, and advanced towards the Capitol Building (figure 1).

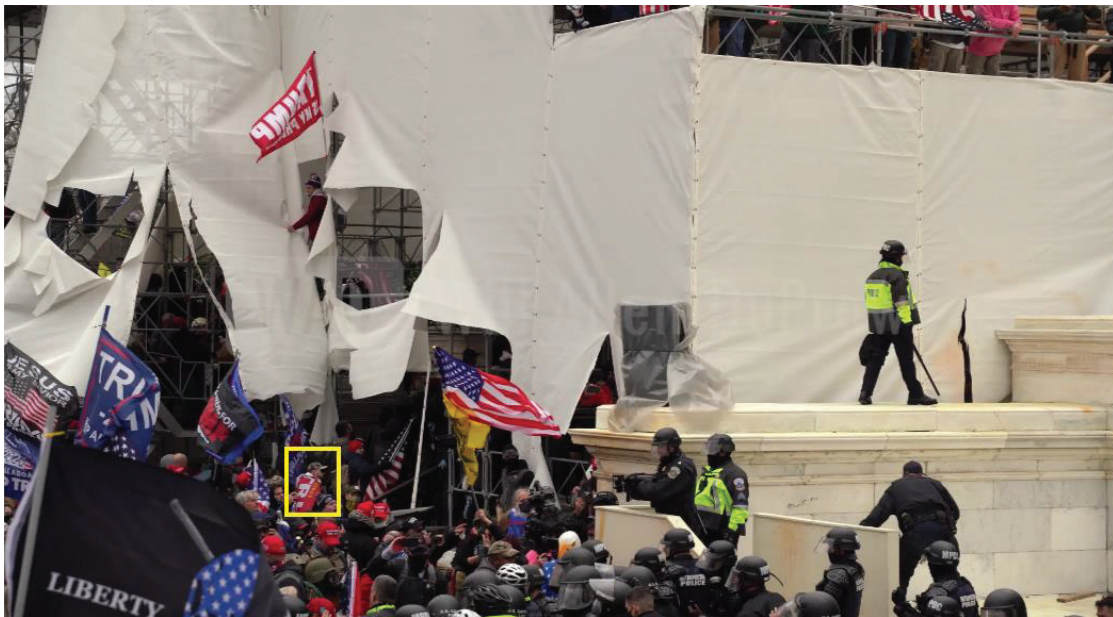


Figure 1

49. BRACKLEY entered the U.S. Capitol via the senate wing doors at 2:23pm, only ten minutes after they were first breached (figure 2). From there, he entered the Crypt, where a large group of rioters had filled the room and pushed against a line of USCP officers (figure 3).

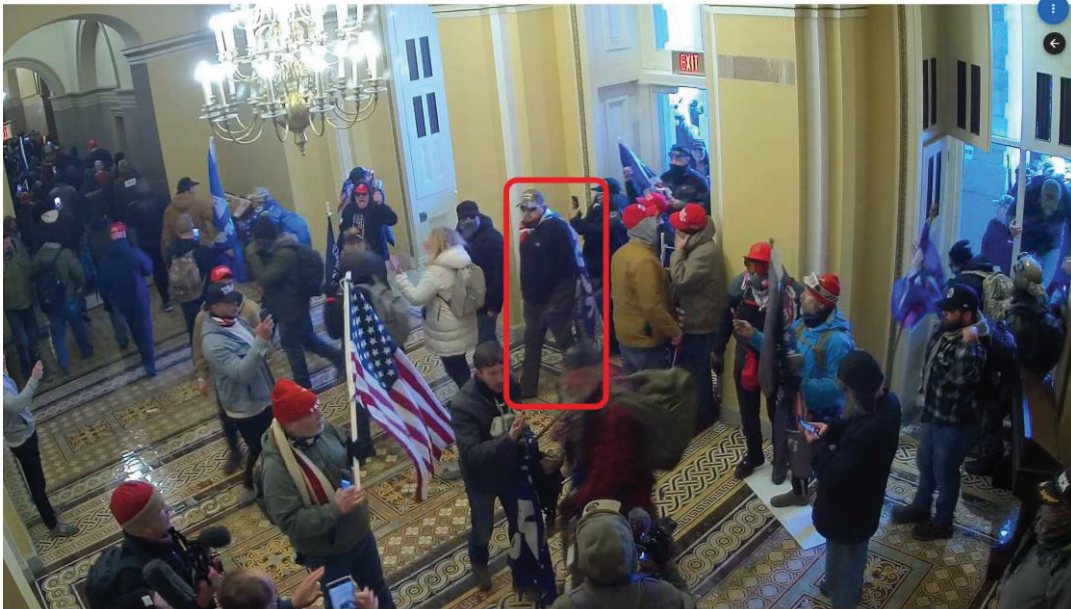


Figure 2



Figure 3

50. The rioters in the Crypt eventually overwhelmed the line of USCP officers, gaining further access to the Capitol. BRACKLEY and several dozen rioters entered a hallway behind the Crypt where they were again stopped by USCP officers. But again, BRACKLEY and the rioters pushed past the officers and continued down the hall (figures 4 & 5).





Figure 4

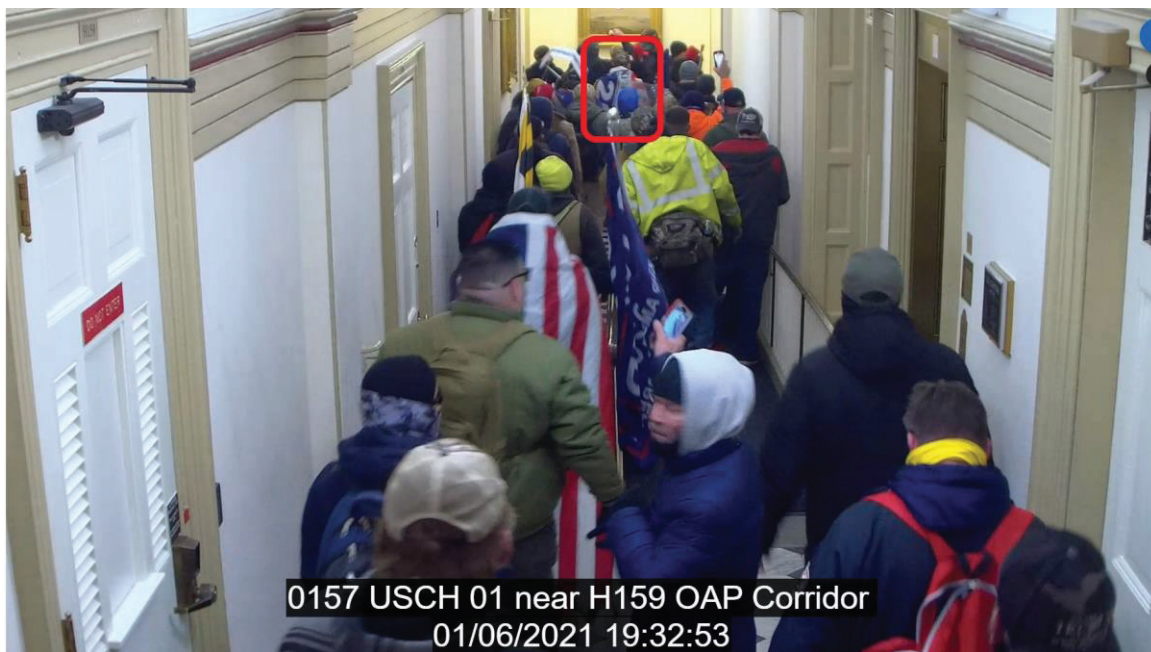


Figure 5

51. BRACKLEY reached and ascended a set of stairs that led to the Rotunda. There he turned North and walked down a hallway toward the Senate Chamber, which had just been evacuated several minutes earlier. As before, BRACKLEY, and others behind him, were stopped

in the hallway by USCP officers. A video posted to “Newsflare” depicts the interaction between BRACKLEY (circled in yellow) and the officers, USCP officers EG and MS (see Figures 6-8 below).

52. The officers told BRACKLEY to “back up” and one officer gave him a small push backwards. Brackley did not retreat, and asked where Pelosi’s office was, as others behind him called her name. About 40 seconds into his conversation with the officers, BRACKLEY turned to the crowd behind him and shouted, “let’s go!” He then then leaned forward and with both arms pushed through the two officers, leading the crowd behind him towards the Senate Chamber (circled in blue in figures 6 and 8).



Figure 6





Figure 7



Figure 8

53. As BRACKLEY led the rioters past USCP officers EG and MS, a group of USCP officers in riot gear entered the hallway from the opposite end (near the Senate Chamber Door) and halted the crowd. Capitol security footage shows BRACKLEY (circled in yellow) leading rioters down the hall as additional USCP officers entered and intercepted them (figure 9). A police



line formed as the rioters pushed against the officers, who tried to back the crowd away from the Senate Chamber (figure 10).



Figure 9



Figure 10

54. For about five or six minutes, a standstill ensued between the rioters and USCP officers in the hallway. Open source footage shows the same standstill, but from the other end of the hallway (see figures 11 and 12 below). BRACKLEY stood among the crowd as others shouted expletives directed at Members of Congress, including, “fuck McConnell.” The rioters then resumed pushing the USCP police officers backwards towards the Senate hallway, while chanting “USA.”



Figure 11



Figure 12

55. One USCP officer deployed chemical spray, causing BRACKLEY and a number of other rioters to retreat. BRACKLEY, appearing to feel the effects of chemical spray, retreated to a stairwell. Other rioters and a law enforcement officer provided BRACKLEY with assistance. BRACKLEY then continued down the stairs into the Crypt, where he turned and continued South. He exited the Capitol through the South Door at 3:05pm, over 40 minutes after first entering the building (figure 13).





Figure 13

*Facts Specific to This Application – The Device(s)*

56. As discussed in paragraphs 40-42, Google location data obtained via legal service showed two devices associated with BRACKLEY and cellular number (207) 837-1238 present at the U.S. Capitol on January 6, 2021.

57. Moreover, a search warrant served on Google for information associated with BRACKLEY's accounts returned photos of BRACKLEY at the U.S. Capitol (figure 14). In the photo, BRACKLEY appears to take a selfie on the West Lawn of the U.S. Capitol. Thus, there is probable cause to believe BRACKLEY used one of these devices, associated with cellular number (207) 837-1238, to record events at the U.S. Capitol.



Figure 14

49. It is well-known that virtually all adults in the United States use mobile digital devices. In a fact sheet from June 12, 2019, The Pew Research Center for Internet & Technology estimated that 96% of Americans owned at least one cellular phone, and that that same 2019 report estimated that 81% of Americans use at least one smartphone. *See* Mobile Fact Sheet, <https://www.pewresearch.org/internet/fact-sheet/mobile/> (last visited Jan. 9, 2021).

50. In my training and experience, it is common for individuals to retain their cell phones for many months or years. I also know, based on my training and experience, that when individuals obtain new mobile phones or update their old mobile phones, they often transfer their data from the old phone to the new phone. Moreover, individuals often back up or preserve copies

of digital media (such as photos and videos) across multiple devices (such as tablets) to prevent loss. Indeed, some companies provide services that seamlessly sync data across devices, such as Apple devices and the Apple iCloud service. Thus, even if BRACKLEY was using a different mobile device on January 6, 2021, there is probable cause to believe that digital media created on that device may be found on any current mobile device(s) (or tablets) associated with the cellular number (207) 837-1238 in BRACKLEY's possession.

51. Further, based on the investigation, numerous persons committing the TARGET OFFENSES possessed digital devices to plan their attendance in Washington D.C. on January 6, 2021, to coordinate with other participants at the gatherings there that day, to take, send, and receive photographs and videos relating to events at the U.S. Capitol and in Washington D.C. on January 6<sup>th</sup>, and to communicate and post on social media and digital forums about the events of January 6<sup>th</sup> after they occurred. This information can: (i) reflect the preparation for, arrangement of, and commission of the TARGET OFFENSES; (ii) identify the subject's presence at locations relevant to the TARGET OFFENSES; (iii) reflect the ownership and use of the cellular telephones by persons involved in the commission of the TARGET OFFENSES; (iv) document meetings and communications between associates and co-conspirators; and (v) demonstrate the subject's planning, preparation, motive, and intent regarding the TARGET OFFENSES.

52. In summation, the execution of a search warrant on the TARGET DEVICE(S) would allow law enforcement to, among other things, evaluate the extent of BRACKLEY's criminal activities on January 6, 2021. Additionally, evidence from the TARGET DEVICE(S) may yield ownership information of the TARGET DEVICE(S). All of the aforementioned information would further constitute evidence of the commission of the TARGET OFFENSES.

### **TECHNICAL TERMS**

53. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. “Digital device,” as used herein, includes the following three terms and their respective definitions:

1) A “computer” means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

2) “Digital storage media,” as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks (“DVDs”), USB flash drives, flash memory cards, and internal and external hard drives.

3) “Computer hardware” means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage



devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

b. “Wireless telephone” (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through “wi-fi” networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional “land line” telephones, computers, and other digital devices. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing Global Positioning System (“GPS”) locating and tracking technology, and accessing and downloading information from the Internet.

c. A “tablet” is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touch-screen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, “wi-fi” networks, or otherwise. Tablets typically contain programs called applications (“apps”), which, like programs on both wireless phones, as

described above, and personal computers, perform many different functions and save data associated with those functions.

D. A “GPS” navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated “GPS”) to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

e. “Computer passwords and data security devices” means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

f. “Computer software” means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

m. “Cache” means the text, image, and graphic files sent to and temporarily stored by a user’s computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website in the future.

p. “Encryption” is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

#### **COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC ANALYSIS**

59. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found within the TARGET DEVICE(S), in whatever form they are found. One form in which such items might be found is data stored on one or more digital devices. Such devices are defined above and include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging

devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Thus, the warrant applied for would authorize the seizure of digital devices or, potentially, the copying of stored information, all under Rule 41(e)(2)(B). Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that there is probable cause to believe that the records and information described in Attachment B will be stored in the TARGET DEVICE(S) for at least the following reasons:

a. Individuals who engage in criminal activity, including trespassing at the U.S. Capitol on January 6, 2021, use digital devices like the Device(s) to prepare or arrange for the commission of criminal activity, communicate with associates and coconspirators regarding criminal activity, or to save and share video and photographic evidence of their criminal activity in order to, among other things, glorify their actions to like-minded individuals.

b. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often “back up” or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph.

c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or

no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensics tools. When a person “deletes” a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve “residue” of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer, smart phone, or other digital device habits.

60. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the Device was used, the purpose of their use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in any of the TARGET DEVICE(S) at issue here because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Device(s), not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user’s intent and the identity of the user.



**METHODS TO BE USED TO SEARCH DIGITAL DEVICES**

61. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Recovery of “residue” of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of

particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting “keyword” search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format (PDF), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital

device users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as “AES-256 encryption” to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, “Hide It Pro,” disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, I request permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

62. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of a premises or the execution of an arrest warrant.

a. Therefore, in searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

1. Law enforcement personnel will, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, transport the TARGET DEVICE(S) to an appropriate law enforcement laboratory or similar facility for review. For all the reasons described above, it would not be feasible to conduct a complete, safe, and appropriate search of any such digital devices at the time of arrest. The digital devices, and/or any digital images thereof created by law enforcement, sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

2. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by “opening,” reviewing, or reading the images or first few “pages” of such files in order to determine their precise contents; “scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic “keyword” searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

3. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover “deleted,” “hidden,” or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the seized digital devices will be specifically chosen to identify the specific items to be seized under this warrant.

#### **BIOMETRIC ACCESS TO DEVICE(S)**

63. The proposed warrant permits law enforcement agents to obtain from the person of BRACKLEY (but not any other individuals present at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s) requiring such biometric access subject



to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s). The grounds for this request are as follows:

64. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

65. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

66. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face.

Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

67. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

68. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

69. As discussed in this Affidavit, I have reason to believe that one or more digital devices, the TARGET DEVICE(S), will be found during the search. The passcode or password that would unlock the Device subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the Device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

70. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

71. Due to the foregoing, if law enforcement personnel encounter any Device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the proposed warrant permits law enforcement personnel to obtain from the aforementioned person(s) the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint scanner of the Device(s); (2) hold the Device(s) in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold the Device(s) in front of the face of the aforementioned person(s) to activate the iris recognition feature, for the purpose of attempting to unlock the Device(s) in order to search the contents as authorized by this warrant.

72. The proposed warrant does not authorize law enforcement to require that the aforementioned person(s) state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s). Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

**CONCLUSION**

73. Based upon the above-referenced facts, I assert that there is probable cause to believe that the TARGET DEVICE(S) contains evidence of the TARGET OFFENSES.

74. Based on the foregoing, I request that the Court issue the proposed search warrant pursuant to Federal Rule of Criminal Procedure 41.

75. I further request that the Court permit the search warrant to be executed at any time once the TARGET DEVICE(S) is contained on the premises of the Federal Bureau of Investigation.


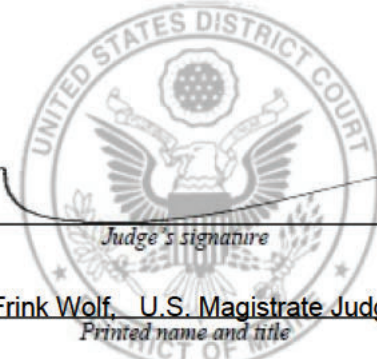
Respectfully submitted,

  
Kurt Ormberg, Special Agent  
Federal Bureau of Investigation

Sworn to telephonically and signed  
electronically in accordance with the  
requirements of Rule 4.1 of the Federal Rules  
of Criminal Procedures

Date: Jul 18 2023

City and state: Portland, Maine

  
  
Judge's signature  
Karen Frink Wolf, U.S. Magistrate Judge  
Printed name and title